Method and circuitry for producing a pseudo random sequence and its use.

Patent Number: EP0624839
Publication date: 1994-11-17
Inventor(s): HESS ERWIN DR RER NAT (DE); SCHRENK HARTMUT DR RER NAT (DE)
Applicant(s):: SIEMENS AG (DE)
Requested Patent: EP0624839, B1
Application Number: EP19940106765 19940429
Priority Number(s): DE19934315544 19930510
IPC Classification: G06F7/58
EC Classification: G06F7/58P1
Equivalents: JP6350409

Abstract

The invention proposes a method and a circuit arrangement for carrying out the method in order to generate a pseudorandom sequence of bit data, using a shift register device (1, 2, 5) with feedback. After a sequence of switching states of the shift register device (1), by means of which it is determined whether the bit data should be output, the bit data are output. The method and the circuit arrangement are preferably used for encrypting data, particularly for the authenticity detection of a data carrier arrangement, for example of chip cards.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Veröffentlichungsnummer: **0 624 839 A1**

(12) EUROPÄISCHE PATENTANMELDUNG

(21) Anmeldenummer: **94106765.4**

(51) Int. Cl.[5]: **G06F 7/58**

(22) Anmeldetag: **29.04.94**

(30) Priorität: **10.05.93 DE 4315544**

(43) Veröffentlichungstag der Anmeldung:
17.11.94 Patentblatt 94/46

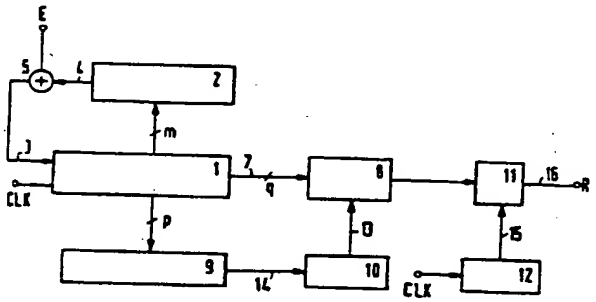
(84) Benannte Vertragsstaaten:
DE FR GB GR IT

(71) Anmelder: **SIEMENS AKTIENGESELLSCHAFT**
Wittelsbacherplatz 2
D-80333 München (DE)

(72) Erfinder: **Hess, Erwin, Dr. rer. nat.**
Meisenstrasse 18
D-85521 Ottobrunn (DE)
Erfinder: **Schrenk, Hartmut, Dr. rer. nat.**
Fasanenweg 22
D-85540 Haar (DE)

(54) Verfahren und Schaltungsanordnung zum Erzeugen einer Pseudozufallsfolge sowie deren Verwendung.

(57) Die Erfindung schlägt ein Verfahren und eine Schaltungsanordnung zur Durchführung des Verfahrens vor, um eine Pseudozufallsfolge von Bitdaten unter Verwendung einer rückgekoppelten Schieberegistereinrichtung (1, 2, 5) zu erzeugen. Nach einer Folge von Schaltzuständen der Schieberegistereinrichtung (1), durch die festgelegt wird, ob eine Ausgabe der Bitdaten erfolgen soll, wird eine Ausgabe der Bitdaten durchgeführt. Das Verfahren bzw. die Schaltungsanordnung wird bevorzugt zur Verschlüsselung von Daten, insbesondere zur Echtheitserkennung einer Datenträgeranordnung, beispielsweise einer Chipkarten, verwendet.



EP 0 624 839 A1

Die Erfindung betrifft ein Verfahren und eine Schaltungsanordnung zum Erzeugen einer Pseudozufallsfolge von Bitdaten unter Verwendung einer rückgekoppelten Schieberegistereinrichtung, bei der durch mindestens einen Schaltzustand festgelegt wird, ob eine Ausgabe der Bitdaten erfolgt.

Pseudozufallsfolgen bzw. pseudozufällige Binärfolgen werden vielfach zur Untersuchung von analogen und digitalen Systemen eingesetzt. Darüber hinaus spielen Pseudozufallsfolgen eine bedeutende Rolle bei der Verschlüsselung von Daten.

Es sind zahlreiche Schaltungsanordnungen bekannt, solche Pseudozufallsfolgen von Bitdaten zu erzeugen. In dem Buch Tietze, Schenk "Halbeiter-Schaltungstechnik", 5. Auflage sind auf den Seiten 509 bis 512 Schaltungsanordnungen beschrieben, um solche Pseudozufallsfolgen zu erzeugen. Zur Erzeugung von Pseudozufallsfolgen verwendet man üblicherweise Schieberegister, die in bestimmter Weise rückgekoppelt sind. Die Rückkopplung wird dabei aus Exklusiv-ODER-Schaltungen zusammengesetzt. Die größte nicht periodische Bitfolge, die ein Schieberegister mit n Stufen erzeugen kann, ist $N = 2^n-1$ Bit lang. So kann mit einem vierstufigen Schieberegister beispielsweise eine Pseudozufallsfolge mit einer maximalen Periodenlänge von 15 Bit erzeugt werden. Eine dafür geeignete Schaltung ist in Abbildung 20.23 der genannten Literaturstelle zu sehen.

Beim Verschlüsseln von Daten wird dagegen die rückgekoppelte Schieberegistereinrichtung mit einer Schlüsselinformation, d.h. ein geheimes Datenwort, beaufschlagt. Mit diesem Datenwort wird festgelegt, an welcher Stelle der Pseudozufallsfolge am Ausgang der rückgekoppelten Schieberegistereinrichtung der Datenstrom der Pseudozufallsfolge beginnt.

Befindet sich beispielsweise in einer tragbaren Datenträgeranordnung, wie z.B. einer Chipkarte, und in einer mit dieser zusammenarbeitenden Datenein-/ausgabeeinrichtung jeweils ein gleiches rückgekoppeltes Schieberegister, und ist der gleiche Schlüssel auf beiden Seiten bekannt, so können die von der einen Datenträgeranordnung zur Datenein/ausgabeeinrichtung verschlüsselt gesendeten Daten wieder entschlüsselt bzw. ein zwischen beiden Seiten ausgetauschter Datenstrom gleichermaßen verschlüsselt und die verschlüsselten Daten verglichen werden. Damit ist unter anderem ein Echheitsnachweis der Chipkarte möglich und ein gewisser Schutz vor Fälschungen bzw. Mißbrauch sichergestellt.

Bisherige Verfahren und Konzepte zur Sicherung solcher Datenträgeranordnung verwenden anstelle einer strengen Echtheitsprüfung zur Ausschaltung von Fälschungen und Mißbrauch die Überprüfung eines durch Nachbauten oder Emulationen nur sehr schwer realisierbaren charakteristischen Merkmals. Bekannt ist darüber hinaus auch die Überprüfung der Gültigkeit der gespeicherten Daten über den Zusatz eines mit dem oben bereits erwähnten geheimen Schlüssel in einer Datenträgeranordnung erzeugten Codes für einen Echtheitsnachweis des Dateninhalts.

Problematisch ist bei diesem bekannten Verfahren, daß die Kontrollsignale abgehört bzw. am Ein/Ausgang der Datenträgeranordnung, beispielsweise der Chipkarte, abgegriffen werden können, wodurch ein Wiedereinspielen der Kontrollinformation zur Fälschungszwecken möglich ist.

Bei elektronischen Schaltungen mit Mikroprozessorarchitektur wird dieser Nachteil durch Einsatz eines kryptografischen Authentifikations- oder Identifikationsvorganges nach dem Prinzip der herausfordernden Frage und dazu passenden Antwort (Challenge und Response-Prinzip) bzw. mit Zero-Knowledge-Protokoll ausgeschaltet.

Dieses Challenge-Response-Prinzip sieht beispielsweise bei einer Chipkarte und einer Datenein-/ausgabeeinrichtung zum Lesen dieser Chipkarte vor, daß zunächst die Datenein-/ausgabeeinrichtung Daten "Challenge" generiert und diese zur Chipkarte sendet. Dort dient diese "Challenge" zur Berechnung einer sogenannten "Response". Diese "Response" wird mittels eines Algorithmusses zum Echtheitsnachweis berechnet und hängt zweckmäßigerweise von weiteren Daten, dem geheimen Kartenschlüssel und z.B. einer weiteren Größe, wie einem internen Zählerstand, ab. Die von der Chipkarte zur Datenein-/ausgabeeinrichtung gesendete "Response" wird in der Datenein-/ausgabeeinrichtung mit dort vorliegenden Daten verglichen. Diese dort vorliegenden Daten werden mit dem gleichen Algorithmus, dem gleichen geheimen Kartenschlüssel, der Challenge und der Zusatzinformation berechnet. Stimmt die Response mit dieser Berechnung überein, so ist die Chipkarte als gültig erkannt. Andernfalls erfolgt ein Abbruch der Datenverbindung zwischen Chipkarte und Datenein-/ausgabeinrichtung. Die eingangs erwähnte rückgekoppelte Schieberegistereinrichtung wird bei diesen bekannten Systemen dazu verwendet, den geheimzuhaltenden Kartenschlüssel in eine längere Pseudozufallsfolge, eine sogenannte Schlüsselstromfolge, zu transformieren. Bei Vorgabe beliebiger Teile der Schlüsselstromfolge muß es einem Angreifer, der den Kartenschlüssel unbefugter Weise berechnen will, unmöglich sein, weitere Teile der Schlüsselstromfolge vorherzusagen. Dies impliziert, daß es ebenfalls unmöglich sein muß, auf den Schlüssel zurückzurechnen. Die bisher bekannten rückgekoppelten Schieberegistereinrichtungen gewähren hierfür bereits einen guten Schutz, sofern die Schieberegistereinrichtung hinreichend lang ist, z.B. 50 hintereinander geschaltete Schieberegisterzellen aufweist.

Aus der noch nicht veröffentlichten deutschen Patentanmeldung mit dem Aktenzeichen P 43 01 279.5 ist bereits ein Verfahren und eine Schaltungsanordnung zum Erzeugen einer Pseudozufallsfolge von Bitdaten unter Verwendung einer rückgekoppelten Schieberegistereinrichtung bekannt, bei der durch mindestens einen Schaltzustand festgelegt wird, ob eine Ausgabe der Bitdaten erfolgt. Es besteht jedoch ein Bestreben dahin, diese bekannten Verfahren mit geringstmöglichen Aufwand noch besser zu sichern. Hier setzt die Erfindung an.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren zum Erzeugen einer Pseudozufallsfolge der beschriebenen Art sowie eine Schaltungsanordnung zur Durchführung des Verfahrens anzugeben, das gegenüber dem bisher bekannten Verfahren und der bekannten Schaltungsanordnung eine höhere Sicherheit aufweist und einfach zu realisieren ist. Darüber hinaus soll eine geeignete Verwendung für dieses Verfahren und diese Schaltungsanordnung aufgezeigt werden.

Diese Aufgabe wird für das Verfahren dadurch gelöst, daß nach einer Folge von Schaltzuständen der Schieberegistereinrichtung eine Ausgabe der Bitdaten durchgeführt wird.

In einer Weiterbildung des erfindungsgemäßen Verfahrens ist es vorgesehen, daß Ausgangssignale der Schieberegistereinrichtung einer nichtlinearen logischen Funktion als Eingangsvariable zugeführt werden, daß ein logisches Ausgangssignal der nichtlinearen logischen Funktion als Taktsignal einer Zählereinrichtung zugeführt wird und daß bei Erreichen eines vorbestimmten Zahlerstandes der Zählereinrichtung ein logisches Signal erzeugt wird, durch daß die Bitdaten aus der Schieberegistereinrichtung ausgegeben werden.

Darüber hinaus können die von der Schieberegistereinrichtung ausgegebenen Bitdatendaten in eine Zwischenspeichereinrichtung übernommen werden, aus der der gespeicherte Wert zu festgelegten Zeitpunkten abgerufen wird. Dies kann wiederum durch eine weitere Zählereinrichtung ausgeführt werden, die bei Erreichen eines vorbestimmten Zählerstandes die Ausgabe steuert.

Die Aufgabe wird für die Schaltungsanordnung dadurch gelöst, daß eine rückgekoppelte Schieberegistereinrichtung (1, 2, 5) eine Vielzahl von hintereinander geschalteten Schieberegisterzellen enthält, daß vorgegebene Schieberegisterzellen ausgangsseitig mit einer eine nichtlineare logische Funktion realisierenden Schaltung (9) verbunden sind, daß der Takteingang einer ersten Zählereinrichtung (10) mit einem Ausgang (14) der Schaltung (9) verbunden ist, daß ein Zwischenspeicher (8) eingangsseitig mit mindestens einer der Schieberegisterzellen verbunden ist, daß ein Taktsteuereingang des Zwischenspeichers (8) von einer einen Zählerstand der ersten Zählereinrichtung (10) dekodierenden Logikeinrichtung gesteuert wird, daß eine Schalteinrichtung (11) mit mindestens einem Ausgang des Zwischenspeichers (8) verbunden ist und daß die Schalteinrichtung (11) von einer einen Schaltzustand einer zweiten Zählereinrichtung (12) dekodierenden Logikeinrichtung gesteuert wird.

In einer vorteilhaften Weiterbildung der erfindungsgemäßen Schaltungsanordnung ist vorgesehen, daß das Schieberegister und die zweite Zählereinrichtung mit der gleichen Taktrate gesteuert werden. Die Logikeinrichtungen zur Dekodierung eines jeweils vorbestimmten Zählerstandes können so ausgeführt werden, daß der Überlauf der jeweiligen Zählereinrichtung dekodiert wird. Darüber hinaus kann die Schalteinrichtung ein Logikgatter sein. Vorzugsweise ist die Wortbreite der zweiten Zahlereinrichtung mindestens doppelt so groß wie die Wortbreite der ersten Zählereinrichtung zu wählen.

Gemäß der Erfindung wird das Verfahren oder die Schaltungsanordnung zur Verschlüsselung bzw. Entschlüsselung von Daten und/oder in einer Datenträgeranordnung, insbesondere Chipkarten mit integrierten Schaltungsanordnungen, zu deren Echtheitserkennung eingesetzt.

Die Erfindung wird im folgenden anhand eines Ausführungsbeispieles in Zusammenhang mit einer Figur näher erläutert.

Die erfindungsgemäße Schaltungsanordnung sieht eine rückgekoppelte Schieberegistereinrichtung 1 vor. Die Schieberegistereinrichtung 1 enthalt eine Vielzahl n von hintereinander geschalteten Schieberegisterzellen. Eine Auswahl von m der n Schieberegisterzellen ist über eine Rückkopplungseinrichtung 2 auf den Dateneingang 3 der Schieberegistereinrichtung 1 rückgekoppelt. Die Rückkopplungseinrichtung 2 führt eine logische Funktion aus. Sie enthält vorzugsweise m-1 Exklusiv-ODER-Schaltglieder mit jeweils zwei Eingangsklemmen und einer Ausgangsklemme. Ein erstes EXOR-Schaltglied ist mit zwei der m rückgekoppelten Schieberegisterzellen verbunden. Die weiteren EXOR-Schaltglieder sind eingangsseitig mit der Ausgangsklemme eines anderen EXOR-Schaltgliedes und einem der rückgekoppelten Schieberegisterzellen verbunden. Das letzte der derart hintereinander geschalteten EXOR-Schaltglieder bildet den Ausgang 4 der Rückkopplungseinrichtung 2. Durch ein weiteres logisches Schaltglied 5, zweckmäßigerweise ein Exklusiv-ODER-Schaltglied, wird ein Eingangssignal E eingekoppelt. Dieses Eingangssignal E kann beispielsweise aus einer Geheiminformation, einer Zufallszahl als Challenge und gegebenenfalls einer Zusatzinformation (z.B. ein Datenspeicherinhalt) gewonnen werden.

Erfindungsgemäß ist mit der Schieberegistereinrichtung ausgangsseitig eine Zwischenspeichereinrichtung 8 verbunden. Die Zwischenspeichereinrichtung

richtung 8 hat die Wortbreite 7, die kleiner oder gleich der Wortbreite der Schieberregistereinrichtung 1 sein kann. Ein Takteingang 13 der Zwischenspeichereinrichtung 8 wird von einem Impuls gesteuert, der aus einer Zählereinrichtung 10 unter Dekodierung eines vorbestimmten Zählerstandes erhalten wird. Zweckmäßigerweise wird dieser Impuls beim Überlauf der Zählereinrichtung 10 erzeugt. Die Zählereinrichtung 10 wird von einer eine nichtlineare logische Funktion realisierenden Schaltung 9 taktseitig gesteuert. In der Schaltung 9 werden die logischen Werte von P Schieberegisterzellen verarbeitet. Die nichtlineare logische Funktion der Schaltung 10 setzt sich zweckmäßigerweise aus logischen Schaltgliedern, wie UND- und ODER-Schaltgliedern zusammen. An die Zwischenspeichereinrichtung 8 ist ausgangsseitig eine Schalteinrichtung 11 angeschlossen. Die Schalteinrichtung 11 wird an einem weiterem Eingang 15 von einer einen vorbestimmten Zählerstand einer weiteren Zahlereinrichtung 12 dekodierenden Einrichtung gesteuert. Vorzugsweise ist der Steuereingang 15 der Schalteinrichtung 11 mit der Überlaufanzeige des Zahlers 12 verbunden. Der Zähler 12 und das Schieberegister 1 werden vom gleichen Taktsignal CLK gesteuert. Vorzugsweise hat die Zahlereinrichtung 12 mindestens die doppelte Wortbreite der Zählereinrichtung 10. Bei einer Wortbreite von etwa 32 Bit der Zählereinrichtung 10 hat der Zähler 12 dann zweckmäßigerweise eine Wortbreite von 64 oder 128 Bit.

Die erfindungsgemäße Schaltungsanordnung arbeitet folgendermaßen: Nach einer definierten Voreinstellung des Schieberegisterzustandes wird das Eingangssignal E, welches wie bereits erwähnt aus einer Geheiminformation, einer Zufallszahl oder gegebenenfalls einer Zufallsinformation bestehen kann, in die rückgekoppelte Schieberegistereinrichtung I eingegeben. Diese Eingabe wird über die Verknüpfungslogik 5, hier ein EXOR-Schaltglied, mit der Rückkopplungsinformation am Ausgang 4 der Rückkopplungseinrichtung 2 verknüpft. Die Schaltung 9 zur Erzeugung der nichtlinearen Funktion erzeugt datenabhängige Zählimpulse an ihrem Ausgang 14, mit denen die Zählereinrichtung 10 hochgezählt wird. Bei Erreichen eines vorbestimmten Zählerstandes, vorzugsweise des Überlaufs des Zählers 10, wird ein Taktimpuls erzeugt, durch den der Zustand des Schieberegisters 1 zumindest teilweise in den Zwischenspeicher 8 übernommen wird. Die Zählrate der Zählereinrichtung 10 ist somit niedriger als die Taktrate des Schieberegisters 1. Bei jedem weiteren Überlauf des Zählers 10 werden die im Zwischenspeicher 8 enthaltenen Daten durch den neuen Zustand der Schieberegistereinrichtung 1 überschrieben. Der Zähler 10 wird dann rückgesetzt und durchläuft erneut den Zählbereich.

Der Zähler 12 läuft datenunabhängig mit de Taktrate des Schieberegisters 1. Wenn der Zählc 12 den vorbestimmten Zählerstand, vorzugsweis: Überlauf, erreicht, wird ein Impuls erzeugt, mit der die Schalteinrichtung 11 freigegeben wird. Die i der Zwischenspeichereinrichtung 8 gespeicherte Bitdaten werden dann als logisches Ausgangssignal R an den Ausgang 16 der Schalteinrichtung 11 weitergegeben. Es hat sich als zweckmäßig erwiesen, für das Schaltglied 11 ein logisches Schaltglied zu verwenden, mit dem ein Bit der Zwischenspeichereinrichtung 8 an den Ausgang 16 bei jedem Überlauf des Zählers 12 ausgegeben wird. Somit ergibt sich für eine Gesamtwortbreite des Ausgangssignals R von r Bit eine Anzahl von r Rechenläufen. Die gesamte Verarbeitungsdauer wird dann durch den Zählbereichs des Zählers 12 bestimmt.

Patentansprüche

1. Verfahren zum Erzeugen einer Pseudozufallsfolge von Bitdaten unter Verwendung einer rückgekoppelten Schieberegistereinrichtung (1, 2, 5), bei der durch mindestens einen Schaltzustand der Schieberegistereinrichtung (1, 2, 5) festgelegt wird, ob eine Ausgabe der Bitdaten erfolgt,
dadurch gekennzeichnet, daß nach einer Folge von Schaltzuständen der Schieberegistereinrichtung (1, 2, 5) eine Ausgabe der Bitdaten durchgeführt wird.

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet, daß Ausgangssignale der Schieberegistereinrichtung (1) einer nichtlinearen logischen Funktion als Eingangsvariable zugeführt werden, daß ein logisches Ausgangssignal der nichtlinearen logischen Funktion als Taktsignal einer Zählereinrichtung (10) zugeführt wird und daß bei Erreichen eines vorbestimmten Zählerstandes der Zählereinrichtung (10) ein logisches Signal erzeugt wird, durch daß die Bitdaten aus der Schieberegistereinrichtung (1) ausgegeben werden.

3. Verfahren nach Anspruch 2,
dadurch gekennzeichnet, daß die Bitdaten durch das von der Zählereinrichtung (10) erzeugte logische Signal gesteuert in einen Zwischenspeicher (8) übernommen werden und daß zu festgelegten Zeitpunkten mindestens ein im Zwischenspeicher (8) gespeichertes Bitdatum ausgegeben wird.

4. Verfahren nach Anspruch 3,
dadurch gekennzeichnet, daß eine weitere Zählereinrichtung (12) mit dem Schieberegi-

stertakt gesteuert wird und daß bei Erreichen eines festgelegten Zählerstandes der weiteren Zählereinrichtung (12) ein logisches Signal erzeugt wird, durch das die Ausgabe aus dem Zwischenspeicher (8) gesteuert wird.

5. Schaltungsanordnung zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 4, **dadurch gekennzeichnet,** daß eine rückgekoppelte Schieberegistereinrichtung (1, 2, 5) eine Vielzahl von hintereinander geschalteten Schieberegisterzellen enthalt, daß vorgegebene Schieberegisterzellen ausgangsseitig mit einer eine nichtlineare logische Funktion realisierenden Schaltung (9) verbunden sind, daß der Takteingang einer ersten Zählereinrichtung (10) mit einem Ausgang (14) der Schaltung (9) verbunden ist, daß ein Zwischenspeicher (8) eingangsseitig mit mindestens einer der Schieberegisterzellen verbunden ist, daß ein Taktsteuereingang des Zwischenspeichers (8) von einer einen Zählerstand der ersten Zählereinrichtung (10) dekodierenden Logikeinrichtung gesteuert wird, daß eine Schalteinrichtung (11) mit mindestens einem Ausgang des Zwischenspeichers (8) verbunden ist und daß die Schalteinrichtung (11) von einer einen Schaltzustand einer zweiten Zählereinrichtung (12) dekodierenden Logikeinrichtung gesteuert wird.

6. Schaltungsanordnung nach Anspruch 5, **dadurch gekennzeichnet,** daß die Taktsignalsteuerungen des Schieberegisters (1) und der zweiten Zählereinrichtung (12) gekoppelt sind.

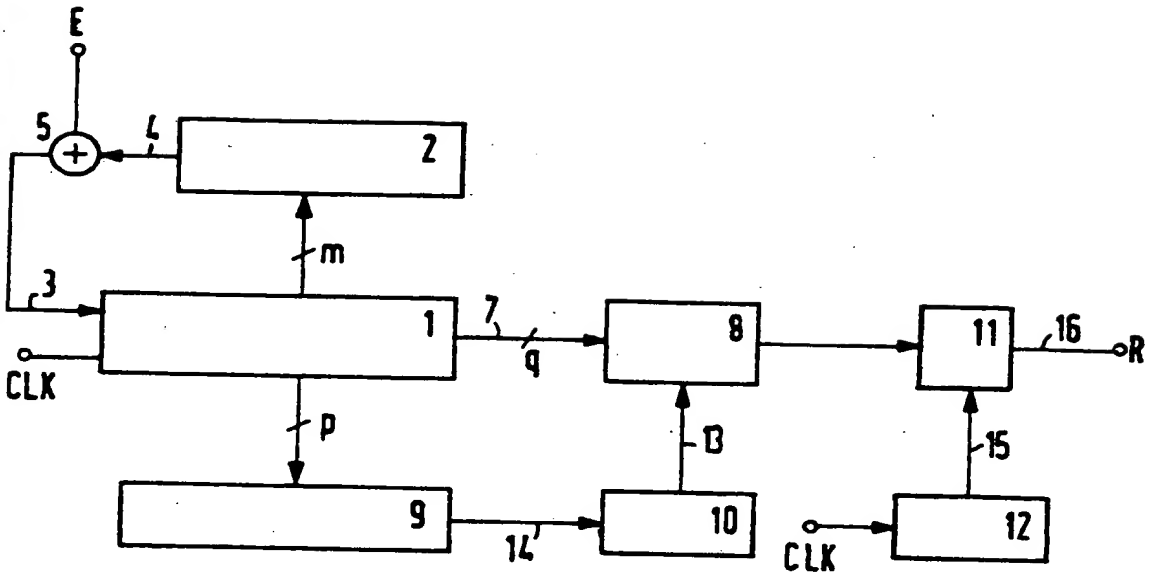
7. Schaltungsanordnung nach Anspruch 5 oder 6, **dadurch gekennzeichnet,** daß die mit der ersten und der zweiten Zählereinrichtung (10, 12) verbundenen Logikeinrichtungen jeweils den Überlauf der ersten bzw. zweiten Zählereinrichtung (10 bzw. 12) dekodieren.

8. Schaltungsanordnung nach einem der Ansprüche 5 bis 7, **dadurch gekennzeichnet,** daß die Schalteinrichtung (11) ein Logikgatter ist.

9. Schaltungsanordnung nach einem der Ansprüche 5 bis 8, **dadurch gekennzeichnet,** daß die Wortbreite der zweiten Zählereinrichtung (12) mindestens das Zweifache der Wortbreite der ersten Zählereinrichtung (10) ist.

10. Verwendung des Verfahrens nach einem der Ansprüche 1 bis 4 oder der Schaltungsanordnung nach einem der Ansprüche 5 bis 9 in einer Datenträgeranordnung, insbesondere einer Chipkarte mit einer integrierten Schaltungsanordnung, zur Echtheitserkennung.

11. Verwendung des Verfahrens nach einem der Ansprüche 1 bis 4 oder der Schaltungsanordnung nach einem der Ansprüche 5 bis 9 zum Verschlüsseln und/oder Entschlüsseln von Daten.


E
5
4
2
m
3
1
7
q
8
11
16
R
CLK
p
13
15
9
14
10
CLK
12